

This will be a 5-minute vote.

The vote was taken by electronic device, and there were—yeas 404, nays 6, answered “present” 6, not voting 17, as follows:

| [Roll No. 404] | | |
|----------------|-----------------|-----------------|
| YEAS—404 | | |
| Abercrombie | Davis, David | Jackson-Lee |
| Ackerman | Davis, Lincoln | (TX) |
| Aderholt | Deal (GA) | Jefferson |
| Akin | DeFazio | Johnson (GA) |
| Alexander | DeGette | Johnson (IL) |
| Allen | Delahunt | Johnson, E. B. |
| Altmire | DeLauro | Johnson, Sam |
| Andrews | Dent | Jones (NC) |
| Arcuri | Diaz-Balart, L. | Jones (OH) |
| Baca | Diaz-Balart, M. | Jordan |
| Bachmann | Dicks | Kagen |
| Bachus | Dingell | Kanjorski |
| Baird | Doggett | Kaptur |
| Baldwin | Donnelly | Keller |
| Barrett (SC) | Doolittle | Kennedy |
| Barrow | Doyle | Kildee |
| Bartlett (MD) | Drake | Kilpatrick |
| Barton (TX) | Dreier | King (NY) |
| Bean | Duncan | Kingston |
| Becerra | Edwards | Kirk |
| Berkley | Ehlers | Klein (FL) |
| Berman | Ellison | Kline (MN) |
| Berry | Ellsworth | Knollenberg |
| Biggert | Emanuel | Kucinich |
| Bilbray | Emerson | Kuhl (NY) |
| Bilirakis | Engel | LaHood |
| Bishop (GA) | English (PA) | Lamborn |
| Bishop (NY) | Eshoo | Lampson |
| Blackburn | Etheridge | Langevin |
| Blumenauer | Everett | Larsen (WA) |
| Blunt | Fallin | Larson (CT) |
| Boehner | Farr | Latham |
| Bonner | Fattah | LaTourette |
| Bono Mack | Feeney | Latta |
| Boozman | Ferguson | Lee |
| Boren | Filner | Levin |
| Boswell | Forbes | Lewis (CA) |
| Boucher | Fortenberry | Lewis (GA) |
| Boustany | Fossella | Lewis (KY) |
| Boyd (FL) | Foster | Linder |
| Boyd (KS) | Fox | Lipinski |
| Brady (PA) | Frank (MA) | LoBiondo |
| Brown (GA) | Franks (AZ) | Lofgren, Zoe |
| Brown (SC) | Frelinghuysen | Lowey |
| Brown, Corrine | Galleghy | Lucas |
| Brown-Waite, | Garrett (NJ) | Lungren, Daniel |
| Ginny | Gerlach | E. |
| Buchanan | Giffords | Lynch |
| Burgess | Gilchrest | Mack |
| Butterfield | Gingrey | Mahoney (FL) |
| Buyer | Gohmert | Maloney (NY) |
| Calvert | Gonzalez | Manzullo |
| Cantor | Goode | Marchant |
| Capito | Goodlatte | Markey |
| Capps | Gordon | Marshall |
| Capuano | Granger | Matheson |
| Cardoza | Graves | Matsui |
| Carnahan | Green, Al | McCarthy (CA) |
| Carney | Green, Gene | McCarthy (NY) |
| Carson | Grijalva | McCaul (TX) |
| Carter | Hall (NY) | McCollum (MN) |
| Castle | Hall (TX) | McCotter |
| Castor | Hare | McDermott |
| Cazayoux | Harman | McGovern |
| Chabot | Hastings (FL) | McHenry |
| Chandler | Hastings (WA) | McHugh |
| Childers | Hayes | McIntyre |
| Clarke | Heller | McKeon |
| Clay | Hensarling | McMorris |
| Cleaver | Herseth Sandlin | Rodgers |
| Clyburn | Higgins | McNerney |
| Coble | Hill | McNulty |
| Cohen | Hinche | Meek (FL) |
| Cole (OK) | Hinojosa | Meeks (NY) |
| Conyers | Hirono | Melancon |
| Cooper | Hobson | Mica |
| Costa | Hodes | Michaud |
| Costello | Hoekstra | Miller (FL) |
| Courtney | Holden | Miller (MI) |
| Cramer | Holt | Miller (NC) |
| Crenshaw | Honda | Miller, Gary |
| Crowley | Huoley | Miller, George |
| Cubin | Hoyer | Mitchell |
| Cuellar | Hunter | Mollohan |
| Culberson | Inglis (SC) | Moore (KS) |
| Cummings | Inslee | Moore (WI) |
| Davis (AL) | Israel | Moran (KS) |
| Davis (CA) | Issa | Moran (VA) |
| Davis (IL) | Jackson (IL) | Murphy (CT) |
| Davis (KY) | | Murphy, Patrick |

| | | |
|---------------|------------------|----------------|
| Murphy, Tim | Ross | Stupak |
| Murtha | Rothman | Sullivan |
| Musgrave | Roybal-Allard | Tanner |
| Myrick | Royce | Tauscher |
| Nadler | Ruppersberger | Taylor |
| Napolitano | Ryan (OH) | Terry |
| Neal (MA) | Ryan (WI) | Thompson (CA) |
| Neugebauer | Salazar | Thompson (MS) |
| Nunes | Sali | Thornberry |
| Oberstar | Sánchez, Linda | Tiahrt |
| Obey | T. | Tiberi |
| Oliver | Sanchez, Loretta | Tierney |
| Pallone | Sarbanes | Towns |
| Pascarella | Saxton | Tsongas |
| Pastor | Scalise | Turner |
| Payne | Schakowsky | Udall (CO) |
| Pearce | Schiff | Udall (NM) |
| Pence | Schmidt | Upton |
| Perlmutter | Schwartz | Van Hollen |
| Peterson (MN) | Scott (GA) | Velázquez |
| Petri | Scott (VA) | Visclosky |
| Pickering | Sensenbrenner | Walberg |
| Pitts | Serrano | Walden (OR) |
| Platts | Sestak | Walsh (NY) |
| Poe | Shadegg | Walz (MN) |
| Pomeroy | Shays | Wamp |
| Porter | Shea-Porter | Wasserman |
| Price (NC) | Sherman | Schultz |
| Pryce (OH) | Shimkus | Waters |
| Putnam | Shuler | Watson |
| Radanovich | Shuster | Watt |
| Rahall | Simpson | Waxman |
| Ramstad | Sires | Weiner |
| Rangel | Skelton | Welch (VT) |
| Regula | Slaughter | Weller |
| Rehberg | Smith (NE) | Westmoreland |
| Reichert | Smith (NJ) | Wexler |
| Renzi | Smith (TX) | Whitfield (KY) |
| Reyes | Smith (WA) | Wilson (NM) |
| Reynolds | Snyder | Wilson (OH) |
| Richardson | Solis | Wilson (SC) |
| Rodriguez | Souder | Wittman (VA) |
| Rogers (AL) | Space | Wolf |
| Rogers (KY) | Speier | Woolsey |
| Rohrabacher | Spratt | Wu |
| Ros-Lehtinen | Stark | Yarmuth |
| Roskam | Stearns | Young (FL) |

NAYS—6

| | | |
|---------------|-----------|------------|
| Campbell (CA) | Herger | Sessions |
| Conaway | King (IA) | Young (AK) |

ANSWERED “PRESENT”—6

| | | |
|-------------|------------|-------------|
| Bishop (UT) | Cannon | Price (GA) |
| Brady (TX) | Davis, Tom | Weldon (FL) |

NOT VOTING—17

| | | |
|-------------|---------|---------------|
| Braley (IA) | Hulshof | Peterson (PA) |
| Burton (IN) | Kind | Rogers (MI) |
| Camp (MI) | Loebach | Rush |
| Flake | McCrery | Sutton |
| Gillibrand | Ortiz | Tancredo |
| Gutierrez | Paul | |

ANNOUNCEMENT BY THE SPEAKER PRO TEMPORE

The SPEAKER pro tempore (during the vote). There are 2 minutes remaining in this vote.

□ 1703

Mr. CONAWAY changed his vote from “yea” to “nay.”

So (two-thirds being in the affirmative) the rules were suspended and the resolution was agreed to.

The result of the vote was announced as above recorded.

A motion to reconsider was laid on the table.

RESOLUTION RAISING A QUESTION OF THE PRIVILEGES OF THE HOUSE

Mr. WOLF. Madam Speaker, pursuant to rule IX, I rise to notify the House of my intention to offer a resolution as a question of the privileges of the House.

The form of my resolution is as follows:

Directing the Chief Administrative Officer and the Sergeant At Arms of the House of

Representatives to take timely action to ensure that all Members, committees, and offices of the House are alerted of the dangers of electronic attacks on the computers and information systems used in carrying out their official duties and are fully briefed on how to protect themselves, their official records, and their communications from electronic security breaches.

Understanding that the Clerk will finish the rest of the resolution, I ask unanimous consent that it be considered as read.

The SPEAKER pro tempore. Without objection, the reading is dispensed with.

There was no objection.

Mr. WOLF. Madam Speaker, I call up the resolution just noticed.

The SPEAKER pro tempore. The Clerk will report the resolution.

The Clerk read as follows:

H. RES. 1263

Whereas beginning in August 2006, several of the computers used by Congressman Frank R. Wolf, a Representative from the Commonwealth of Virginia, in carrying out his official and representational duties were compromised by an outside source;

Whereas the Chief Administrative Officer of the House of Representatives, acting through House Information Resources (HIR), alerted Congressman Wolf to this incident and cleaned and returned the compromised computers to the Congressman's office;

Whereas since this attack, it has been discovered that computers in the offices of other Members, as well as in the office of at least one committee of the House, have been similarly compromised;

Whereas in subsequent meetings with HIR and officials from the Federal Bureau of Investigation, the outside source responsible for these incidents was revealed to be located in the People's Republic of China;

Whereas according to HIR, when Members use Blackberry devices or cell phones while traveling overseas, especially in nations in which access to information is tightly controlled by the government, they are at risk of having their conversations or other personal information recorded or collected without authorization;

Whereas HIR, the FBI, and the House Security Office briefed the affected offices on the security breaches that have occurred, and have done a good job in attempting to protect other offices of the House from similar threats; and

Whereas it is nevertheless not clear that all Members, committees, and other offices of the House are aware of the existing threats against the security and confidentiality of the electronic records of their offices or their overseas electronic communications, nor is it clear that Members and other House personnel have been fully briefed on how to protect themselves, their official records, and their communications from electronic security breaches: Now, therefore, be it

Resolved, That the Chief Administrative Officer and the Sergeant at Arms of the House of Representatives, in consultation with the Director of the Federal Bureau of Investigation, should take timely action to ensure that all Members, committees, and offices of the House are alerted of the dangers of electronic attacks on the computers and information systems used in carrying out their official duties and are fully briefed on how to protect themselves, their official records, and their communications from electronic security breaches.

The SPEAKER pro tempore. The resolution qualifies.

Pursuant to the rule, the gentleman from Virginia (Mr. WOLF) and the gentlewoman from California (Ms. ZOE LOFGREN) each will control 30 minutes.

The Chair recognizes the gentleman from Virginia.

Mr. WOLF. I yield myself such time as I may consume.

(Mr. WOLF asked and was given permission to revise and extend his remarks.)

Mr. WOLF. Madam Speaker, in August 2006, four of the computers in my personal office were compromised by an outside source. This source first hacked into the computer of my Foreign Policy and Human Rights staff person, then the computers of my Chief of Staff, my Legislative Director and my Judiciary Committee staff. On these computers was information about all the case work I've done on behalf of political dissidents and human rights activists around the world. That kind of information, as well, everything else on my computer, e-mails, memos, correspondence and district case work, was open for outside eyes to see.

I'm aware that the computers in the offices of several other Members of the Congress were similarly compromised, as well as a major committee, the Foreign Affairs Committee. That means the computers in the House Foreign Affairs Committee have been compromised. It is logical to assume that critical and sensitive information about U.S. foreign policy and the work of Congress to help people who are suffering around the world, was also open to view from those official computers.

In subsequent meetings with the House Information Resources and the FBI, it was revealed that the outside sources responsible for this attack came from within the People's Republic of China. Just so it's understood, they acknowledged that this attack came from within the People's Republic of China.

The cyber attacks permitted the source to probe our computers to evaluate our systems defenses and to view and copy information. My suspicion is some say that I perhaps was targeted by the Chinese sources because of the history of speaking out about China's abysmal, very abysmal human rights record.

My offices' computers were cleaned and returned to me by House Information Resources, but ever since this happened, I've been deeply concerned that this institution, the institution of the United States Congress, is definitely not adequately aware of or protected from these types of threats.

I've also learned that this threat exists not only here in the Capitol complex, but also when Members travel overseas. I've been told that, particularly in countries in which access to information is tightly controlled by the government, Members are at risk of having their conversations and information recorded or stolen from their cell phones and Blackberry devices. That means, when a Member of the

House, the Senate or the administration goes abroad, goes to China, everything, and if they use their cell phone or they use their Blackberry, it's being recorded by the Chinese government. And I don't believe any Member of the Congress has been told of that.

As I've shared my office experience with other Members, it has become clear to me that many Members and committees of other offices in the House do not fully understand the extent of the threat against the security of their offices and how to protect themselves.

I have no information to confirm this, but it would be realistic that the Senate may also be at risk.

The committees in both Chambers on Government Reform, Intelligence, the Judiciary Committee, the Armed Services and the Homeland Security should have hearings on this issue. This is an issue that must have public hearings, as well as closed door and private hearings.

That is why, Madam Speaker, I'm here today on the House floor. I'm speaking out about the threat of cyber attacks from China and other countries on the entire U.S. government, including our military, because of my deep concern about maintaining the security and the integrity of our government.

According to a report from the Congressional Service, and I quote, "U.S. counterintelligence officials reportedly have stated that about 140 different foreign intelligence organizations regularly attempt to hack into the computer systems of U.S. government agencies and U.S. companies."

□ 1715

This happens with alarming frequency, according to a recent Business Week article entitled "The New Espionage Threat." This article states that U.S. Government agencies reported almost 13,000 cyber security incidents in fiscal year 2007, triple the number from just 2 years earlier.

The May 31 cover story of the National Journal, the respected National Journal, says, "The Chinese Cyber-Invasion," and every Member should read it, titled the "Chinese Cyber-Invasion" reported, "Electronic devices by the U.S. Commerce Secretary Carlos Gutierrez and his party during a December 2007 visit to China were invaded using spyware that could steal information." Gutierrez was in China with a high-level delegation to discuss trade-related issues.

Now, this Congress said it's concerned about trade-related issues with China, and that's why he was there, such as intellectual property rights, consumer product safety, and market access. The Associated Press also reported on the breach. Why did we learn about this in the press instead of from our own government officials? Did our government do anything about this attack? Did they get information from Secretary Gutierrez that could be used

against American business in negotiation of trade agreements?

China, in particular, is actively engaged in espionage against the United States. I recently had the opportunity to read, and I hope every Member of the Congress has read, the U.S.-China Economic Security Review Commission's classified report—it is in the House Intel Committee—to the Congress and found the report's conclusions to be very alarming. The report addresses China's activities in the areas of espionage, cyber warfare, and arms proliferation. I strongly urge all Members of the House to read this report as it gives a clear picture of the threat that China poses, the threat, and in their words, that China poses to our national security.

In fact, the Pentagon's 2008 annual report to Congress stated that "in the past year, numerous computer networks around the world, including those owned by the U.S. Government, were subject to intrusions that appear to have originated within the People's Republic of China."

According to the Business Week article in 2007, the U.S. Government launched a classified operation called Byzantine Foothold to combat sophisticated new attacks that were compromising sensitive information at the State Department and a defense contractor, such as Boeing, the source of which U.S. officials allege is China.

The Business Week article states that computer attacks have targeted sensitive information on the Internet works of at least several Federal agencies: the Defense Department, the State Department, the Energy Department, the Commerce Department, the Health and Human Services Department, and the Agriculture Department, and the Treasury Department. Defense contractors Boeing, Lockheed Martin, General Electric, Raytheon, and General Dynamics have also been targeted.

Despite everything we read in the press, our intelligence and law enforcement, national security, and diplomatic corps remain hesitant to speak out on the problem. Perhaps they are afraid that talking about the problem will reveal our vulnerability. In fact, I have been urged not to speak out about this threat. But our adversaries already know we are vulnerable. Pretending that we are not vulnerable is a mistake.

As a Nation, we must decide when we are going to start considering this type of activity a threat to our national security and the men and women who serve in the Armed Forces, a threat that we must confront and which we must protect ourselves.

Madam Speaker, the apparent lack of national urgency to address this problem only gives those who wish us harm an extra advantage.

The Government Accounting Office reported in 2007 that no comprehensive strategy exists yet to coordinate improvements of computer security across the Federal Government in the private sector.

I strongly believe that the appropriate officials, including those of the Department of Homeland Security and the FBI, should brief all Members of Congress in a closed session regarding threats from China and other countries against security of House technology including our computers, BlackBerry devices, and phones. There must be a session where any Member who is interested has the opportunity to get briefed by the FBI and the Department of Homeland Security and others.

The potential for massive and coordinated cyber attacks against the United States is no longer a futuristic problem. We must prepare ourselves now and develop procedures for responding to this threat. Members need to know how best to protect themselves, their staff, and their official business from these threats. I have experienced this threat firsthand, as have others in the Congress, and are deeply worried that this institution, the United States Congress, is not adequately protected.

Congress should take the lead in protecting our government and indeed our country from the threat posed by cyber espionage activities.

James Lewis, the director of the Technology and Public Policy Program at the Center for Strategic and International Studies remarked last year in testimony before the House committee on Homeland Security that "If gangs of foreigners broke into the State or Commerce Department and carried off dozens of file cabinets, there would be a crisis. When the same thing happens in cyberspace, we shrug it off as another of those annoying computer glitches we must live with."

The apparent complacency in both the private and public sectors toward this threat is astonishing. We must know about the threat. We must speak out about how to protect ourselves and form a comprehensive strategy with which to respond.

Stephen Spoonamore, a CEO of a cyber security firm called Cybrinth, put the matter succinctly in the National Journal article. He said, "By not talking openly about this, they are making truly a dangerous national security problem worse . . . Secrecy in this matter benefits no one. Our Nation's intellectual capital, industrial secrets, economic security are under daily and withering attack. The oceans that surround us are no protection from sophisticated hackers, working at the speed of light on behalf of nation-states and mafias."

We must cease, Madam Speaker, this Congress must cease, the administration must cease denying the scope and scale and risk of the issue. And he goes on to say a growing number of his peers "believe that our Nation is in grave and growing danger."

Mr. Spoonamore is right. We are making this dangerous national security problem worse by not discussing it openly. I believe this institution, as my resolution states, should get the facts, and armed with these facts, should

take the necessary action to protect the safety and integrity of the House.

In 1789, Madam Speaker, British Parliament member William Wilberforce, speaking to his colleagues about the slave trade, said, "having heard all of this, you may choose to look the other way, but you can never again say you do not know."

This Congress on both sides of the aisle and people in the administration can never again, can never again say you do not know; and the American people should ask their Members of Congress, Do you know and what are you going to do about it.

We cannot afford to look the other way when foreign sources are threatening to compromise our government institutions, our economy, our very way of life through cyber espionage. We cannot sit by and watch. I urge the adoption of the resolution.

I reserve the balance of my time.

Ms. ZOE LOFGREN of California. Madam Speaker, I yield myself such time as I may consume.

I will note that I have had a chance to discuss this resolution with Congressman WOLF. At the conclusion of our discussion, we will refer this resolution to the House Administration Committee where we will do the appropriate follow-up, and I personally plan to keep in touch with the author of the resolution so that the concerns that he has are fully addressed.

I will just note that when the new majority was elected to the House and I was then appointed to the House Administration Committee, one of the first things I did was to ask to be briefed on our cyber security situation in the House. And I did receive that report. Certainly some things had been done. But more, in my judgment, needed to be done, and we have followed through on that.

I will say that both the Speaker and Leader BOEHNER have met with the House computer security officials and were told that the sophisticated technology that we do have in place is going to prevent and detect intrusions, but it depends on Members doing what they need to do to work within our security environment.

We have security system programs in place that safeguard against unauthorized system access and disclosure of data, system controls that are in place to identify, verify trace authorized and unauthorized user activity, and to prevent unauthorized modification or destruction of House data.

Chairman BRADY has ordered an immediate implementation of additional protections. He's also directed House personnel to work with the FBI and other security agencies to ensure that necessary steps are taken to safeguard House systems. These improvements will help ensure that House network and data remains protected from harm.

In addition to these efforts, the House has instituted a working-smarter series, and we have had actually briefings for staff in the congressional

offices asking those staff in Member offices to come in and become aware of the cyber security steps that they need to take in each Member's office. I don't know that every Member has had full staff participation in that, and in discussing this with Mr. WOLF, it would be my intention, perhaps working with Mr. LANGEVIN who is chairing the Homeland Security Subcommittee on Cyber Security, to ask the Democratic caucus and the Republican conference to meet and to highlight this issue so Members will know.

I mean, some Members know all about it, and apparently some Members didn't know enough about it; and I'll take that admission very seriously.

What more do we need to do? Well, we have sophisticated firewalls in place today that monitor all incoming network traffic. We have an intrusion-detection system, and we have multiple anti-virus and spyware programs. That's important because you want redundancy and overlap. You don't want to rely on just one system. We also have—you may have seen in some of the hallways—teams monitoring wireless systems. It's a kind of antenna they're waving around. They're trying to detect unauthorized wireless setups that are a potential problem for our security.

What further can we do?

Well, we have tried to insist that Members use more vigorous passport protection schemes. And one of the things we're looking at is instead of asking Members, forcing Members to do that. Now we get pushback when Members are told what to do in their individual offices, but I think that's one of the things that we need to talk about.

Another thing we're looking at, and this was an issue in the intrusion mentioned a minute ago, is whether we're updating our virus software and whether the patches to this software have been uploaded. And Members don't do it. A lot of times Members just neglect to do it. If you don't put the patches in, you're just bare. So we're thinking about maybe centralizing that function. Again, some Members may not like that, but you've got it one way or the other. I mean, you can't be concerned about intrusion if we don't take the steps necessary to actually protect ourselves.

We also are looking at additional encryption efforts, enhancing our real-time monitoring by the security office, and potentially implementing a digital rights management scheme.

Now, I just want to talk a little bit about Member responsibility.

If Members are going to access Web sites in China, you're engaging in risky behavior, and it may be necessary for some Members who are monitoring human rights to do that. I accept that. But it is not a good idea to visit a Web site in China with the computer that's networked with all of your sensitive data on board because if you do, you're going to get malware, and you are

going to lose your data to whoever has put that malware on the site.

So I would strongly suggest, and this is a teachable moment, that if Members feel a need to monitor Web sites in China and other countries, that they get a laptop, get an air card, don't put any other sensitive data on it and monitor to your heart's content, but don't leave yourself vulnerable to your data being removed.

□ 1730

No doubt there are root kits, there are bot nets that are going to be infecting your computer and potentially even turning them into zombie computers. Additional things that we want to look at is data leakage protection and some security assessments which is actually going underway right now.

Just a word on cyber security generally, which Mr. WOLF has mentioned. In the 108th Congress, I had one of the best experiences in my congressional career of serving with MAC THORNBERRY who chaired the Cyber Security Subcommittee. I was the ranking member, and we worked really hard that Congress together. I think it was the only subcommittee, the end of the Congress, we didn't have majority report and a minority report. We had one report that reflected both of our views, and the view was that the Federal Government was way behind in what we needed to do on cyber security.

I remain a member of the Homeland Security Committee. I serve under Mr. LANGEVIN's chairmanship on the committee with cyber security jurisdiction. We have had many, many public hearings, in addition to classified briefings, on the real deficiencies in our cyber security environment in the Federal Government, and I will tell you, I am frustrated to this very moment that so little has been done to keep us safer. Frankly, the House of Representatives has much more robust cyber security than the Department of Homeland Security. That's kind of a chilling thought, but unfortunately, it is true.

So, at this point, I recognize the gentleman's concern. I certainly plan on working with you, and I also want to make sure that each and every Member of this House understands the environment, what their responsibilities are, what their staffs' responsibilities are, understand what we've done as an institution, and what the tradeoffs are going forward in terms of even more vigorous protection.

With that, I reserve the balance of my time.

Mr. WOLF. Before I yield the gentleman 5 minutes, I would say this is bigger than just the House, though. The computers of the House have been violated and when Members go abroad, but also, it deals with people in the administration.

And so I think there need to be public hearings by the Armed Services Committee and by the Judiciary Committee. This Congress is never reluctant to hold a hearing on different

things. This is a major issue so it must be broader than just the House Administration Committee.

I yield 5 minutes to the gentleman from New Jersey.

Mr. SMITH of New Jersey. I thank my good friend for yielding.

Madam Speaker, in December of 2006 and then again in March of 2007, my Human Rights Subcommittee's computers were attacked by a virus that, in HIR's words, "intended to take control of the computers." At that time, the IT professionals cleaned the computers and informed my staff that the attacks seemed to come from the People's Republic of China. They said it came through or from a Chinese IP address. The attackers hacked into files related to China. These contained legislative proposals directly related to Beijing, including the Global Online Freedom Act, e-mails with human rights groups regarding strategy, information on hearings on China—I chaired more than 25 hearings on human rights abuses in China—and the names of Chinese dissidents. While this absolutely doesn't prove that Beijing was behind the attack, it raises very serious concern that it was.

Like Mr. WOLF, I too speak out often against the systematic abuse of human rights by the Chinese Communist government, whether it be religious persecution, the systematic use of torture, the total absence of labor rights, press freedom or free speech, and since 1979, the pervasive use of forced abortion to implement the barbaric one-child-per-couple policy, the gravest violation of women's and children's rights ever. So I was deeply concerned that the perpetrators of these crimes searched the China files on my computers.

It is now coming to light, Madam Speaker, that some other Members may as well have been attacked, and more needs to be done to combat this danger. So I thank my friend for offering this very important resolution.

Madam Speaker, cyber attacks on Congress are only a small, but not insignificant, part of a much larger pattern of attacks to which the executive branch, the Pentagon, and American business is the chief target. I want to recommend, as my colleague Mr. WOLF did a moment ago, "The Chinese Cyber-Invasion," an eye-opening feature article that recently appeared in the National Journal. There we learn that some of our top cyber security experts believe that Chinese hackers have already shown that they can hack down our power grid. The experts believe that the Chinese hackers have caused power blackouts in the U.S. One blackout in 2003 was the largest in U.S. history and affected some 50 million people.

Chinese hackers and cyber warriors are mapping U.S. government and commercial networks at a rate that in the last 18 months has increased exponentially. A high-level ODNI official has referred to "a kind of cyber militia . . . coming in volumes that are just stag-

gering," he said. The same official said that what makes the Chinese hackers stand out "is the pervasive and relentless nature of the attacks."

Madam Speaker, with enormous aid, comfort and scads of one-of-a-kind technological assistance from U.S. companies, including Microsoft, Cisco, Google and Yahoo, the Chinese Government has achieved a huge qualitative capability to suppress freedom of speech on the Internet at home and to wage cyber warfare abroad.

Two years ago, I chaired the first congressional hearing on this unseemly, dangerous partnership, an alliance that enables the Chinese secret police to find, arrest, incarcerate, and torture religious believers and pro-democracy activists in China. Google, for its part, has become the de facto center for China's ubiquitous anti-American, anti-Tibetan, anti-religious propaganda machine, while Cisco has made the dreaded Chinese secret police among the most effective in the world.

I have introduced the Global Online Freedom Act, which has cleared all three committees of jurisdiction and is ready for floor action, and I, again, respectfully ask the leadership to bring it to the floor to combat this ever-worsening threat. For the Chinese people, it will make the prospect of freedom and democracy more achievable. For Chinese dissidents, it's a matter of survival, and for us, it may inhibit the transfer of technologies that we must prevent from falling into the hands of the enemies of fundamental human rights.

Mr. WOLF's resolution is a wake-up call, and it alerts us to take more effective action and thwart disruption and the theft of sensitive data. I strongly support the resolution.

Ms. ZOE LOFGREN of California. Madam Speaker, I would like to yield to the chairman of the subcommittee with jurisdiction over cyber security on the House Homeland Security Committee, Mr. LANGEVIN, 5 minutes.

(Mr. LANGEVIN asked and was given permission to revise and extend his remarks.)

Mr. LANGEVIN. I want to thank the gentlelady for yielding, and I also want to thank the gentleman from Virginia for bringing this serious issue to light.

As chairman of the Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology, I have spent much of the 110th Congress focused on issues of information security. In fact, my subcommittee has held eight hearings and conducted investigations into dozens of cyber security issues. And while I believe we have made some real progress in the last year or so, we still have a lot of work ahead of us.

I fully agree with Director of National Intelligence, Mike McConnell, when he says that cyber security is the most significant national security issue facing the Nation today, and it's easy to understand why.

We rely on computers in every aspect of our lives, from our banking systems

and our electric grid, to our military and the functions of our Government. And whether we realize it or not, each of us is dependent on the effective functioning of computers. For many years, these systems were largely closed to the outside world, but in the Internet age, this is no longer true.

In the history of the world, never have so many people had so much access to ideas, knowledge, and skills. Unfortunately, never before have so many people also possessed the capability to cause such catastrophic economic and physical harm to the United States.

Now, this is not a hypothetical threat. In 2007, Vice Chairman of the Joint Chiefs of Staff James Cartwright told Congress that "America is under widespread attack in cyberspace." And though we have not seen the massive denial of service attacks that the Nation of Estonia experienced last year, the Federal Government and the private sector have been the victims over the last decade of an extensive and deliberate espionage campaign that has had a significant impact upon our Nation.

As Major General William Lord stated publicly last year, "China has downloaded 10 to 20 terabytes"—again 10 to 20 terabytes—"of data from the DOD's unclassified network." That's the equivalent of almost half of the Library of Congress.

American businesses, too, have been dramatically affected. One estimate suggests that our companies lose an estimated \$70 billion each year due to cyber crime, and individual citizens are far from immune either. Electronic identity theft affects, as you know, millions of us every year.

There are a variety of motives for these attacks, but the result is clear: the weakening security and economic stability of our country. National security is a nonpartisan issue, and we must all work together to commit the resources and the manpower necessary to respond to this threat.

The situation raised by Congressman WOLF today illustrates that while the House of Representatives has strong information protections in place, cyber security threats pose a challenge to computer systems everywhere, and it is an ever-evolving and dynamic threat. And we need to do all we can to stay out in front of it and ahead of it.

Now, I'm pleased that the House leadership takes this issue very seriously and is taking action to ensure that House systems are properly secured, and I especially commend House Administration Chairman BOB BRADY for directing the Chief Administration Officer to immediately adopt additional protections for House computers.

I also want to commend the gentlelady from California (Ms. ZOE LOFGREN) for her due diligence and passion about cyber security as well, and I certainly appreciate the working relationship, good working relationship, that she and I have together.

I am ready to do anything I can to help ensure that our House information systems are as secure as possible. Recognizing that this issue is much larger than the House of Representatives, I am also committed to addressing the broader issues of cyber security across the Federal domain and the national critical infrastructure.

I look forward to working with my colleagues to ensure that our Federal Government is educated and prepared at all levels to thwart cyber attacks and protect the integrity of our networks.

Mr. WOLF. I recognize the gentleman from Illinois (Mr. KIRK), a member of the Appropriations Committee whose computer was also stripped from someone in China, for 1½ minutes.

Mr. KIRK. I want to thank the gentleman from Virginia for this resolution.

In my judgment, most Members of Congress are quite naive about the security of their offices against an expert cyber attack from a foreign intelligence service.

With regards to China, these types of attack are uniquely damaging to the U.S.-China relationship. While the resolution before us concerns breaches in the security of House computers, we can assume that the Senate is also under attack.

The message we would send to China is that such a cyber attack on the Congress poses unique dangers to the long-term relationship of China and the United States. We all know that a Member of Congress will soon be sworn in as a President of the United States in just 7 months. To the senior leaders overseas that may direct such a cyber attack against congressional offices, I would ask, What are you thinking? The intelligence gained would pale in comparison to the damage directly done to U.S.-China relations.

House Information Systems should dramatically upgrade the protection of U.S. computers, especially in the House, and offer Members secure Blackberries to protect against that unique vulnerability. We should also review other security procedures that should lead the Congress especially to increase the protection of the White House, the Defense Department, and the State Department.

I want to commend my colleague Mr. WOLF for bringing this to the attention of the House and especially the attention of the American people.

Ms. ZOE LOFGREN of California. Madam Speaker, just a couple of comments.

In terms of protecting ourselves, I can't emphasize enough, it is important for all of us to take steps to secure ourselves.

I had an opportunity to take a look. We keep track of this, the intrusions. I took April by example. The origin of the intrusion in April, the country that originated the largest number of intrusions into the House, the United States of America.

□ 1745

And China wasn't second. So yes, there are intrusions coming from China, from Russia, from European countries, from our own country, and we'd better take precautions to protect our data.

You can't protect a BlackBerry. If you take your BlackBerry overseas—I just thought everyone knew this—and download something, you are opening yourselves up to a vulnerability. Now, we can take a snapshot of where your BlackBerry is before you go and see if it's been compromised while you're gone, but if you're not secure in your activities, you're not secure in your activities.

And so I take very seriously what you're saying, which is that not every Member understands this. We have to change that, and I'm going to be active in playing my part to change that.

Mr. SMITH of New Jersey. Will the gentlewoman yield?

Ms. ZOE LOFGREN of California. I will yield to the gentleman.

Mr. SMITH of New Jersey. I appreciate my friend for yielding.

One of the concerns is, while they may be terrorists or homegrown, we're talking about and we are very concerned about is that this is the Government of the People's Republic of China and their enablers, people who are part of a network, that is very much focused on trying to wreak havoc and to glean information about dissidents, about legislative strategy, and about what we know about what's going on—

Ms. ZOE LOFGREN of California. Reclaiming my time, let me just note that obviously we don't want sensitive information from the government to be in the hands where it can be compromised. We're not arguing that. I'm just pointing out that if Members use a computer in their office that's networked to visit a Web site in China, you can bet—you're asking for some malware to be put on your computer, and it's going to take everything that is accessible to the other computers in your network. And so you shouldn't do that.

When I travel with my laptop, and I sometimes do, you know, I never hook that laptop into the network of the House. In fact, it's against the rules to do so. And I don't do it because that would compromise the computer network. And so I would just note that the Homeland Security Committee has been very vigorous over the past 5 or 6 years that I'm aware of, I mean, we don't need a wake-up call, we've been yelling "fire" for half a decade and we haven't really been heard by those who have responsibility in the administration to act. However, we are moving forward in terms of systems in the House.

What I'm hearing from you, Mr. WOLF, and others, is that Members' level of information is quite variable on this, and we will take that seriously and do an effort of outreach on that.

Madam Speaker, I reserve the balance of my time.

Mr. WOLF. Madam Speaker, I recognize the gentleman from Virginia (Mr. FORBES) for 2 minutes.

Mr. FORBES. Thank you, Congresswoman WOLF.

Madam Speaker, I rise in support of the privileged resolution offered by my good friend from Virginia, but I just want to make clear of one thing. This is not just about computers in the House of Representatives. This is about computers and information technologies all across the country.

China is among the most aggressive countries spying on the United States. The FBI has stated that China is and will continue to be America's greatest counterintelligence problem during the next 10 to 15 years.

FBI Director Mueller has testified before House committees that China's intelligence collection in the U.S. is substantial and ongoing. The extent of Chinese espionage operations targeting the United States should worry every single Member that we have here.

And Madam Speaker, the reason it's so important is they don't use the same techniques that a lot of countries do, they use a much wider scope. And we understand that economic and industrial espionage cost American businesses nearly \$60 billion in 2005.

Director Mueller has stated that China has established more than 3,000 front companies in the United States whose purpose is to conduct espionage on Americans. And America's national security, intellectual property secrets, trade secrets, and infrastructure secrets are all at considerable risk.

If you look at your own computers, and not just the illegal access, but next to the United States, the largest number of hits that my computer has in my office is from China; 14,000 hits. I guarantee you I don't have many constituents that are residing in Beijing, but it could have something to do with the fact that I serve on the Armed Services Committee and chair the China Caucus.

Let me give you two other examples. Chi Mak was a Chinese spy who worked for a United States defense contractor. In 2005, an FBI wiretap caught him discussing how to smuggle an encrypted computer disk to China that had intelligence information that could potentially jeopardize the U.S. Navy.

Secondly, we had Katrina Leung, which public sources have indicated operated as a double agent for China and the United States and contaminated probably two decades worth of U.S. intelligence relating to China as well as crippling the FBI's Chinese counterintelligence program.

She accessed such sensitive intelligence through entrapment of a senior FBI agent. Both examples illustrate serious threats to America's security, and they're the ones we know about from public sources.

I have introduced H.R. 3806, the SPIES Act, to help strengthen penalties against these serious foreign espionage threats. We cannot

continue to fight today's espionage threats with yesterday's laws. Yet while we continue to name post office after post office in this body we can't find the time to consider this legislation.

Mister Speaker, we must be mindful of the dangers of dismissing a known, ongoing security threat. Turning a blind eye will not address this issue, and I appreciate my colleague for calling our attention to this important issue that affects the House of Representatives and the country at large. I fully support the resolution and urge my colleagues to do the same.

Ms. ZOE LOFGREN of California. Madam Speaker, I would just note, the thrust of the gentleman's resolution has to do with the House, which is why I'm addressing the House computers. On the other hand, I've been concerned for a long time about cyber security in the Federal Government, in the DOD, in the Homeland Security Department, and frankly, in the private sector. And it is very spotty.

I just wanted to make a correction. I was briefed on the National Journal story. What happened on the nuclear power plant issue, it was not an attack. It was someone who was uploading some software onto a computer that he did not realize was networked, and it was inconsistent with other software. And actually it didn't work as designed because the control system shut it down.

Having said that, I have said in public—so I don't mind saying it here again today—that we have cyber security vulnerabilities, especially SCADA systems that were installed years ago before we were thinking about security. We have not paid enough attention to that either in the private sector or the public sector.

We have had FERC before the Committee on Homeland Security on several occasions urging them to force utilities to take the steps they need to preserve their networks, and they say two things: One, they don't have enough authority; and two, they don't want any more authority. So we've said this is an emergency situation, and we're not getting an emergency response attitude from the agencies with authority.

That is certainly something that other committees may want to look at. I'm just familiar with the efforts that I've been involved in, and they've been substantial, although, regrettably, not yet successful.

I would just like to stand up a little bit for our IT guys here in the House. It was our IT guys who discovered that your computers had been infected and notified you. And it's bad that they were infected, but it's part of the price you pay when you use a network computer to visit a potentially dangerous Web site. But they cleaned it up and responded promptly, and I think they deserve credit for letting that system work.

And just a final note on hits from China. That's not the same as an attack. And we keep track of the hits we have on our Web site. I mean, I get hits

on my Web site from all over the world. I don't know why people in other countries come and visit my Web site, but it's not an attack, it's that they're looking at information that I have made publicly available.

What we are concerned about is attempted intrusions, and there are many of those in an astoundingly small successful effort. This is a constant battle. As the hackers become more sophisticated, our defenses need to become more sophisticated, and it never ends. That's why the effort to improve our patches in our security needs to happen every single day. There needs to be continuous monitoring of our systems. And it has to be all of us. This has to be a team. And every Member needs to take responsibility for this, along with the government itself.

Madam Speaker, I reserve the balance of my time.

Mr. WOLF. Madam Speaker, may I inquire as to how much time I have remaining?

The SPEAKER pro tempore. The gentleman from Virginia has 9 minutes remaining.

Mr. WOLF. Madam Speaker, I yield 4 minutes to the gentleman from Michigan, the ranking member on the Intelligence Committee, Mr. HOEKSTRA.

Mr. HOEKSTRA. I thank my colleague.

One of the jobs that I have here in the Congress is to serve as the ranking member on the Intelligence Committee, also having served as the chairman on the Intelligence Committee.

Today I rise in support of Congressman WOLF's privileged resolution on cyber security to salute him for his efforts to educate this House and the American public about the growing threat to U.S. commerce, our national security, and the privacy of the American people.

Unfortunately, some on the other side have attempted to scare the American people into thinking that the gravest threat to their privacy comes from our Nation's hardworking intelligence professionals. That's absolutely not true. Mr. WOLF, in this resolution today, reminds us that the real threat to America's privacy and the safety of Americans comes not from within, but from those who would do us harm from overseas.

Mr. WOLF had the misfortune to personally experience this fact when computers in his office were compromised by hackers from China, the Chinese, in 2006. I agree with my friend from Virginia that his office computers probably were targeted because of his long record of speaking out against human rights violations in China.

While I can't discuss the specifics of what we know, I can tell you that the leadership of this Congress, Republicans and Democrats, are well aware of the cyber espionage threat that exists. But what has this Congress done? Instead of working to modernize and strengthen our Nation's surveillance capabilities, the Democratic leadership

of this Congress has sought to tie the process down in bureaucracy, in red tape. Some have sought to vilify the intelligence professionals we ask to form the first line of our Nation's defense.

And in some cases, instead of talking about the threat to America's privacy posed by foreign cyber espionage and hackers, they instead point the finger of accusation at our intelligence professionals and innocent patriotic businesses that may at this point be helping to protect the Nation, the very same intelligence professionals and businesses we may turn to to help protect our Nation from the cyber threat.

The threats we face are real. These are not just simple viruses, these are sophisticated attacks on a new electronic battlefield. They jeopardize America's security—politically, economically, and militarily. It's a global problem with multiple threats. Some of my colleagues have talked about earlier, there has been reports about what Russia did in Estonia. We know what countries have done against the United States.

So Congress does need to face this and face this issue very seriously. Congress needs to ask tough questions about trade and technology deals involving Chinese finance and businesses. One of the things that we know, while my colleague brings up China in this instance, and the Chinese, we know that it is a global threat. But specifically about China the message is very, very clear, consistently over and over the Chinese cheat.

We also need to focus on the real threats our Nation faces, not those imagined for partisan gain. And most importantly, and most urgently, again, to make sure that our intelligence professionals on the front lines have the tools that they need to keep us safe and to attack this cyber threat, this Congress needs to pass the Senate FISA bill now. Because this law not only affects how we track the radical jihadists who threaten us, it will also impact how we confront the cyber threat as well.

This is a very sophisticated problem, it is a very serious problem. I congratulate my colleague for bringing it forward. This is an issue that I believe we can work on a bipartisan basis. We need to work on a bipartisan basis. But we need to do first things first, and the first thing we need to do now is get FISA passed, and do it soon.

Mr. WOLF. Madam Speaker, I recognize the gentleman from Michigan (Mr. EHLERS) for 2 minutes.

Mr. EHLERS. I thank the gentleman from Virginia for yielding, and I especially thank him for bringing this issue to the floor.

I also thank my colleague from California, who works with me on the House Administration committee, for her very perceptive comments on this problem.

I would just like to add a little historical insight. I was asked by the new

Speaker, Newt Gingrich, some years ago—in 1995 to be exact—to take charge of setting up the new computer system for the House of Representatives. It was a formidable task. And one issue I emphasized over and over was the need for adequate security.

□ 1800

We did the best we could at that time. And I was very proud for a number of years that although the White House got hacked, the Pentagon got hacked, the Senate got hacked, we did not get hacked. Those days are over. And every Member of this House of Representatives has to recognize that.

This is going to involve, first of all, the best possible technology fix. There's no question about it. But there's another aspect that was mentioned by my colleague from California, and that is training Members and staff on how to deal with this threat and this danger. That is not easy.

When I computerized the House, I had to educate my colleagues about computers. It was hopeless. I eventually taught computer classes myself to my colleagues to try to get them interested and to begin using computers. We are going to have to be that direct, that formidable and persistent in ensuring that our colleagues and all our employees understand the threat and that they learn how to deal with the threat and especially learn how to prevent incursions by the actions that they take with their computers and the way they handle their equipment.

This is a major issue. I will pledge, as my colleague from California does, that we will attempt our best to address this on the House Administration Committee, and we will certainly do everything possible to solve it. But it is going to require the vigilance of every employee of the House of Representatives and the Senate for that matter.

Ms. ZOE LOFGREN of California. I will just say that I appreciate Mr. EHLERS' comments. As he has, I have introduced many Members to the concept of the Internet. Luckily that is no longer as necessary today as it was at one time. But some of our colleagues are real white-out-on-the-screen folks, and we need to bring them forward to the modern era.

But you are right. It is not just the Members. As I have mentioned to Mr. WOLF, I have made a commitment that I intend to follow through to ask the Republican Conference and also the Democratic Caucus to appear, not just by myself, but with top-level experts, to explain to Members their responsibilities and vulnerabilities for them when they travel abroad with mobile devices as well as their desktops in their office and how to preserve their network. And it's not just for the staff. I mean how many of us have made clear to the summer interns that if they have their laptop, and they're on a peer-to-peer network for whatever

reason at home, and then they plug that laptop into the House network, I might add in violation of our rules, that they have introduced a vulnerability to our system? I don't know how many of us have given that little tutorial to these wonderful young people, but all of us should.

So I think this has been a helpful resolution, Mr. WOLF, because it has opened my eyes to the need to get Members to pay more attention. And I am going to play the most positive role I can to make sure that happens. But it is also going to take the cooperation of the Members themselves, because if this is not taken seriously, it won't happen.

I reserve the balance of my time.

Mr. WOLF. How much time do I have left, Mr. Speaker?

The SPEAKER pro tempore (Mr. McNULTY). The gentleman from Virginia has 3 minutes remaining.

Mr. WOLF. I thank the gentlelady for her agreement. I think we have to, one, read the National Journal. This is a very respected magazine. And this is a serious problem. Up until now, it has been neglected by many in the administration and many in Congress.

Secondly, I think the American people are ahead of this Congress. And quite frankly on this issue with China, I think they are ahead of the administration. They are ahead of the administration on human rights, religious freedom, persecution and bad goods coming in from China. This Congress and this administration ought to wake up.

Thirdly, people are not anxious to talk about this in the Congress, nor are they anxious to talk about it in the administration. They are not anxious to talk about it. There was an effort to have me not go ahead with this using different techniques and different ideas. And we complied. We worked with the majority every way we can.

I want to say this. I will not let this issue rest. I may not be the fastest person in this institution. But I am as dogged as anyone. And I expect the leadership, I expect the leadership to deal with this not just by the House Administration Committee, I expect the leadership to deal with this on the Armed Services Committee. I expect the leadership to deal with this with regard to the House Intelligence Committee. I expect the Government Operations, has the Government Operations Committee ever been reluctant to hold a hearing on anything? And the answer is "no." They must deal with this issue. And I tell the gentlelady, who has been very good, and I thank her for that, that if this is not resolved, I will be down here on the floor. I will rework this resolution. It will be a privileged resolution. And the next time there will be a vote on this. And then the American people, the American people can see how aggressive this administration and this Congress will be on a major national security issue and the issues of religious freedom and persecution. Keep in mind that 35 Catholic

bishops are in jail in China. Two hundred Protestant pastors are in jail in China. They have plundered the Tibetans, and they're persecuting the Uighurs. This is not a government that is very friendly. And also they are the leading supporter of genocide in Darfur.

With that, knowing this will be dealt with, I reserve the balance of my time.

Ms. ZOE LOFGREN of California. Mr. Speaker, I just want to say that I serve on three committees. I serve on the House Administration Committee. And I am here today in that capacity. I serve on the Homeland Security Committee where I have participated in I would say dozens of hearings on cybersecurity at least over the years. And I serve on the House Judiciary Committee where we have had, we have a little bit of jurisdiction, but we have actually worked pretty hard on our spyware issues and cybersecurity issues. We have paid attention to that.

I know that the Armed Services Committee has also paid attention to the whole issue of cyber warfare and cybersecurity. The Intelligence Committee isn't allowed to tell the rest of us mere mortals who don't serve what they have done, but I certainly hope they are taking this seriously and believe that they are.

I know that the gentleman has the right to close. I would just say that I would like to provide to Mr. WOLF the material from the many, many hearings that we have had. I think that he would value seeing what we have done so far. And also it would be valuable to him to see what remains to be done.

As I said earlier, we have been yelling, actually yelling about this. We have, as a Nation, tremendous vulnerabilities. And you can't always know. You can detect, unless it is spoofed, where an intrusion is coming from. You can't always say who has initiated that intrusion. But I will tell you, these intrusions and hackers are coming from all over the world with all kinds of intentions. And we all ought to take all of this very seriously. And we have failed, I think, to do all of the things that we could have done.

We have worked with the private sector. And at this point, the private sector is so wary of the Department of Homeland Security that there is a reluctance, actually, to work with the department because the information provided to the department will be so insecure. So we have a long ways to go.

I am glad that the gentleman has a strong interest in this. I wish that every Member had a strong interest in it. And maybe after we are through having these presentations to the Republican Conference and the Democratic Caucus, we will have a higher level of Member interest. And maybe instead of just our few voices in the wilderness here in the House, Mr. EHLERS, Mr. LANGEVIN, myself and Mr. THORNBERRY, who have been working on this for so many years, will have more voices, and maybe we will have a better response. I certainly hope so.

I yield back the balance of my time. Mr. WOLF. Mr. Speaker, I yield back the balance of my time.

MOTION TO REFER OFFERED BY MS. ZOE LOFGREN OF CALIFORNIA

Ms. ZOE LOFGREN of California. Mr. Speaker, I have a motion at the desk. The SPEAKER pro tempore. The Clerk will report the motion.

The Clerk read as follows:

Ms. Zoe Lofgren of California moves that the House refer the resolution to the Committee on House Administration.

The SPEAKER pro tempore. Without objection, the previous question is ordered on the motion to refer.

There was no objection.

The SPEAKER pro tempore. The question is on the motion to refer.

The motion was agreed to.

A motion to reconsider was laid on the table.

PROVIDING FOR CONSIDERATION OF H.R. 6063, NATIONAL AERONAUTICS AND SPACE ADMINISTRATION AUTHORIZATION ACT OF 2008

Mr. HASTINGS of Florida. Mr. Speaker, by direction of the Committee on Rules, I call up House Resolution 1257 and ask for its immediate consideration.

The Clerk read the resolution, as follows:

H. RES. 1257

Resolved, That at any time after the adoption of this resolution the Speaker may, pursuant to clause 2(b) of rule XVIII, declare the House resolved into the Committee of the Whole House on the state of the Union for consideration of the bill (H.R. 6063) to authorize the programs of the National Aeronautics and Space Administration, and for other purposes. The first reading of the bill shall be dispensed with. All points of order against consideration of the bill are waived except those arising under clause 9 or 10 of rule XXI. General debate shall be confined to the bill and shall not exceed one hour equally divided and controlled by the chairman and ranking minority member of the Committee on Science and Technology. After general debate the bill shall be considered for amendment under the five-minute rule. It shall be in order to consider as an original bill for the purpose of amendment under the five-minute rule the amendment in the nature of a substitute recommended by the Committee on Science and Technology now printed in the bill. The committee amendment in the nature of a substitute shall be considered as read. All points of order against the committee amendment in the nature of a substitute are waived except those arising under clause 10 of rule XXI. Notwithstanding clause 11 of rule XVIII, no amendment to the committee amendment in the nature of a substitute shall be in order except those printed in the report of the Committee on Rules accompanying this resolution. Each such amendment may be offered only in the order printed in the report, may be offered only by a Member designated in the report, shall be considered as read, shall be debatable for the time specified in the report equally divided and controlled by the proponent and an opponent, shall not be subject to amendment, and shall not be subject to a demand for division of the question in the House or in the Committee of the

Whole. All points of order against such amendments are waived except those arising under clause 9 or 10 of rule XXI. At the conclusion of consideration of the bill for amendment the Committee shall rise and report the bill to the House with such amendments as may have been adopted. Any Member may demand a separate vote in the House on any amendment adopted in the Committee of the Whole to the bill or to the committee amendment in the nature of a substitute. The previous question shall be considered as ordered on the bill and amendments thereto to final passage without intervening motion except one motion to recommit with or without instructions.

SEC. 2. During consideration in the House of H.R. 6063 pursuant to this resolution, notwithstanding the operation of the previous question, the Chair may postpone further consideration of the bill to such time as may be designated by the Speaker.

The SPEAKER pro tempore. The gentleman from Florida is recognized for 1 hour.

Mr. HASTINGS of Florida. Mr. Speaker, for the purpose of debate only, I yield the customary 30 minutes to my colleague and friend from Florida, Representative DIAZ-BALART. All time yielded during consideration of the rule is for debate only.

I yield myself such time as I may consume. I also ask unanimous consent, Mr. Speaker, that all Members be given 5 legislative days in which to revise and extend their remarks on House Resolution 1257.

The SPEAKER pro tempore. Is there objection to the request of the gentleman from Florida?

There was no objection.

Mr. HASTINGS of Florida. Mr. Speaker, House Resolution 1257 provides for consideration of H.R. 6063, the National Aeronautics and Space Administration Authorization Act of 2008, under a structured rule.

The rule provides 1 hour of general debate controlled by the Committee on Science and Technology. It also waives all points of order against consideration of the bill except clauses 9 and 10 of rule XXI.

The rule makes in order the 12 amendments listed in the Rules Committee report accompanying the resolution. Finally, the rule provides one motion to recommit with or without instructions.

□ 1815

Mr. Speaker, the National Aeronautics and Space Administration Authorization Act is a commonsense and fiscally responsible authorization plan for NASA that will strengthen our ability to improve our Nation's economy, communities and programs, as well as our national security.

The bill authorizes \$20.21 billion for NASA for fiscal year 2009. This includes \$1 billion in funding to accelerate the development of the Orion Crew Exploration Vehicle and Ares 1 Crew Launch Vehicle. This ensures that we do not lose ground to Russia and China as we work to build the next generation of space flight vehicles.